the institute

VOLUME 39 • ISSUE 1 • MARCH 2015 • THEINSTITUTE.IEEE.ORG

SPECIAL REPORT

CYBERSECURITY

THWARTING ATTACKS

IEEE

Calendar & IEEE Events

March

4
1962
The **first nuclear power plant in Antarctica** begins operation, in McMurdo Sound.

7–8
Region 10 meeting in Dhaka, Bangladesh.

15
1915
Thomas J. Watson is named president of the Computing-Tabulating-Recording Co. (later IBM), a position he would hold until 1956.

22
1960
IEEE Life Fellows Charles H. Townes and Arthur L. Schawlow receive a patent for the **optical and infrared maser** [pictured with Townes, above].

28–29
Region 2 meeting in Columbus, Ohio, and Region 8 meeting in Limassol, Cyprus [above].

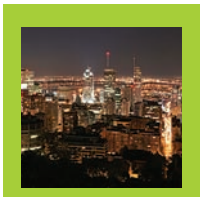
April

6
1957
Hundreds of people take one last trip on **New York City's trolley cars** [above] as they make their final runs.

10–12
Region 3 meeting in Fort Lauderdale, Fla.

11
1900
The **U.S. Navy acquires its first submarine** propelled, once submerged, by electric motors.

15–19
Region 5 meeting in New Orleans.

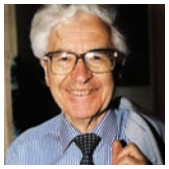


23–26
Region 7 meeting in Montreal.

30
1916
Birth date of IEEE Fellow **Claude E. Shannon**, who became known as the father of information technology.

May

1
1964
John G. Kemeny and Thomas E. Kurtz run **the first program in BASIC**, the computer language they created as a teaching tool.



11
1924
Birth date of **Antony Hewish** [above], corecipient of the 1974 Nobel Prize in Physics for his contribution to the discovery of pulsars, cosmic objects that emit pulses of radio waves.

27
1933
First day of Chicago's **Century of Progress International Exposition** [above]. New technologies on display include air-conditioning, ultraviolet lights, and a voice-controlled model train.

30
1987
Philips Co. introduces the compact disc video (CD-V), a format that could store both video and audio files.

Historical events are provided by the IEEE History Center. For photos and videos of these engineering milestones, visit http://theinstitute.ieee.org/briefings/calendar.

CLOCKWISE FROM TOP: MARTY LEDERHANDLER/AP PHOTO; REX FEATURES/AP PHOTO; HEDRICH BLESSING COLLECTION/ CHICAGO HISTORY MUSEUM/GETTY IMAGES; ISTOCKPHOTO(2); AP PHOTO; ISTOCKPHOTO; COVER: BONNIE NANI

BRIEFINGS

Mildred Dresselhaus

Medal of Honor Goes to Dresselhaus

IEEE LIFE FELLOW Mildred Dresselhaus is the recipient of the 2015 IEEE Medal of Honor "for leadership and contributions across many fields of science and engineering." She is the first woman to receive IEEE's highest award.

Dresselhaus is a professor emeritus at MIT, which she joined in 1960 as a researcher in its Lincoln Laboratory Solid State Division, in Lexington, Mass. She studied the properties of carbon there, and her pioneering research earned her the nickname "Queen of Carbon Science." She became a professor of electrical engineering in 1967, joined the physics department in 1983, and became an Institute Professor of electrical engineering and physics in 1985.

Dresselhaus has made pioneering contributions to the study of phonons, thermal transport in nanostructures, and the structure of carbon nanotubes.

She served in 2000 as director of the U.S. Department of Energy Office of Science, in Washington, D.C. From 2003 to 2008, she was chair of the governing board of the American Institute of Physics. She was president of the American Physical Society in 1984 and of the American Association for the Advancement of Science in 1997 and treasurer of the National Academy of Sciences from 1988 to 1992.

She was presented with the 2014 U.S. Presidential Medal of Freedom, the country's highest honor for civilians, for "deepening our understanding of condensed matter

DONNA COVENEY

systems and the atomic properties of carbon—which has contributed to major advances in electronics and materials research."

The Medal of Honor is sponsored by the IEEE Foundation. Dresselhaus is to receive the award at the annual IEEE Honors Ceremony, to be held 20 June at the Waldorf Astoria Hotel in New York City.

—Amanda Davis

Meet the 2016 Candidates

THE IEEE BOARD of Directors has nominated Senior Member Karen Bartleson and Life Fellow Frederick "Fred" Mintzer as candidates for 2016 IEEE president-elect. They are set to face off in the annual election later this year. The winner will serve as IEEE president in 2017.

Bartleson is senior director of corporate programs and initiatives at Synopsys, an electronic design automation company in Mountain View, Calif. Her responsibilities include creating programs for technical standards development and software tool interoperability, building relationships with universities and research institutions worldwide, and engaging customers with social media. She joined Synopsys in 1995 as manager of its standards group and was director of quality from 2000 to 2002.

Karen Bartleson

Frederick "Fred" Mintzer

CLOCKWISE FROM TOP LEFT: JOHNNY WILSON PHOTOGRAPHY; ISABEL SOLANO/GETTY IMAGES; BARBARA SANTAGATA

She received the 2003 Marie R. Pistilli Women in Electronic Design Automation Achievement Award. Bartleson also authored a book, *The Ten Commandments for Effective Standards: Practical Insights for Creating Technical Standards*, published by Synopsys Press in 2010.

She was president of the IEEE Standards Association in 2013 and 2014. As president, she led the development of a new strategic plan; furthered OpenStand, a set of principles for developing global standards; and finalized IEEE's membership in the Global Standards Collaboration, a volunteer organization that promotes cooperation and collaboration in communications standards development.

As a member of the IEEE Board of Directors in 2013 and 2014, Bartleson chaired and led the development of the strategic plan for the IEEE Internet Initiative Committee, which aims to boost IEEE's influence in the areas of Internet governance, cybersecurity, and policy development. She was also a member of the IEEE Strategy Committee, overseeing the development of IEEE's role in global public policy.

Mintzer joined IBM in 1978 and spent the early part of his career there investigating signal and image processing. He later managed projects that developed image-based digital library technologies and applied them to joint projects with museums and libraries, including the Egyptian Museum, in Cairo; the Hermitage Museum, in Saint Petersburg, Russia; and the Vatican Library, in Vatican City. From 2001 to 2005 he was senior manager of IBM's visual technologies department, which worked on computer graphics, data visualization, and digital imaging.

From 2005 to 2013 he was program director for IBM's Blue Gene Watson supercomputer facility and associate director of its Deep Computing Institute, both at the company's T.J. Watson Research Center, in Yorktown Heights, N.Y. He retired on 1 January 2014.

Mintzer has received more than 25 patents and written more than 50 technical papers. He was twice named an IBM Research Master Inventor.

Mintzer was vice president of IEEE Technical Activities in 2012 and director of Division IX in 2008 and 2009. He was 2009 chair of the IEEE Employee Benefits and Compensation Committee and has been on several other committees, including the IEEE Nominations and Appointments, Governance, and Investment committees. In 2009 he served as Region 1 liaison to the IEEE Technical Activities Board.

He was president of the IEEE Signal Processing Society in 2004 and 2005. As president, he helped launch the society's *IEEE Transactions on Information Forensics and Security*.

—A.D.

Proposed Amendment to the IEEE Constitution

THE IEEE BOARD of Directors has proposed revisions to the IEEE Constitution designed to update the document and accomplish the following:

- better define IEEE membership
- eliminate operational procedures that are currently well defined in, or more appropriate for, the IEEE bylaws or other lower-level governing documents
- better define the roles of the IEEE Assembly and its delegates, which are separate from the roles of IEEE directors, as detailed in the bylaws
- create a closer tie to IEEE's Certificate of Incorporation, the document that legally establishes the organization
- change the voting requirement for amending the constitution to

INSIDE

ONLINE

Available 6 March at theinstitute.ieee.org

A HISTORY OF HACKING
The Institute explores more than a century of hacking incidents.

MEMBERSHIP STATISTICS
Find out which IEEE groups showed the most growth in 2014.

IN MEMORIAM
IEEE honors the lives of three members who recently died.

at least two-thirds of those voting in an annual election, removing the current requirement of achieving a 10 percent return rate of ballots

The Board of Directors endorsed the proposed amendment at its August 2014 meeting and asks the members to vote yes on the proposed amendment, which will be a part of the 2015 IEEE annual election ballot.

To adopt this amendment, an affirmative vote of at least two-thirds of all ballots cast is required, provided the total number of those voting is at least 10 percent of all IEEE's members who are eligible to vote.

More details on the revisions are available at http://www.ieee.org/elections. To read the procedure on how to oppose proposed revisions (IEEE Policies, Section 13.7), visit http://www.ieee.org/about/corporate/governance/index.html.

—Parviz Famouri, IEEE Secretary

Five Elected to the Board

THE IEEE ASSEMBLY in November elected five officers to the IEEE Board of Directors for 2015.

Four of the five, who began serving one-year terms on 1 January, are new officers: Parviz Famouri, secretary; Jerry L. Hudgins, treasurer; Wai-Choong "Lawrence" Wong, vice president, Member and Geographic Activities; and Sheila Hemami, vice president, Publication Services and Products. Saurabh Sinha was elected to serve a second year as vice president, Educational Activities.

—A.D.

REGION NEWS

REGION 1

NORTHEASTERN UNITED STATES

- Student branch formed at **Fairfield University, Connecticut.**
- Student branch at the **University of Maine, Orono,** forms IEEE Power & Energy Society chapter.
- **Berkshire (Massachusetts) Section** forms IEEE Life Member affinity group.
- **Green Mountain (Vermont) Section** forms IEEE Power & Energy Society chapter.

REGION 2

EASTERN UNITED STATES

- Student branch at the **University of Delaware, Newark,** forms IEEE Women in Engineering (WIE) affinity group.

REGION 3

SOUTHEASTERN UNITED STATES

- Student branch at **Georgia Tech** forms IEEE Engineering in Medicine and Biology Society chapter.

REGION 4

CENTRAL UNITED STATES

- Student branch at **Purdue University, West Lafayette, Ind.,** forms IEEE Robotics and Automation Society chapter.

REGION 5

SOUTHWESTERN UNITED STATES

- Student branch formed at the **University of Houston.**

REGION 6

WESTERN UNITED STATES

- Student branch at **San José State University, California,** forms IEEE Signal Processing Society chapter.

REGION 7

CANADA

- **Kingston (Ontario) Section** forms IEEE Power Electronics Society chapter.
- Student branch at the **University of Calgary, Alberta,** forms joint chapter of IEEE Industry Applications and IEEE Power & Energy societies.

REGION 8

EUROPE, MIDDLE EAST, AND AFRICA

- Student branch formed at **Zewail City of Science and Technology, Giza, Egypt.**
- **Hungary Section** forms IEEE Young Professionals (YP) affinity group.
- **Iraq Section** forms IEEE Computational Intelligence Society chapter.
- Student branch formed at the **University of Basilicata, Potenza, Italy.**
- Student branch formed at **Al-Hussein Bin Talal University, Ma'an, Jordan.**
- **Switzerland Section** forms IEEE Education Society chapter.
- Student branches in Tunisia at **National Engineering School of Gabès, National Engineering School of Monastir,** and **National Institute of Applied Science and Technology** form IEEE Industry Applications Society chapters.

REGION 9

LATIN AMERICA

- Student branch at **Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, Brazil,** forms IEEE Robotics and Automation Society chapter.
- **Chile Section** forms IEEE Signal Processing Society chapter.
- **Colombia Section** forms IEEE YP affinity group.
- Student branch formed at **Universidad Surcolombiana, Neiva, Colombia.**
- Student branches formed in Mexico at **Universidad Politécnica de Puebla, San Pedro Cholula,** and **Instituto Tecnológico de La Paz.**
- Student branch at **Universidad de Ingeniería y Tecnología, Barranco, Peru,** forms IEEE Industry Applications Society chapter.
- Student branch at the **University of Piura, Peru,** forms IEEE WIE affinity group.

REGION 10

ASIA AND PACIFIC

- Student branch formed at the **University of Technology, Sydney.**
- **Western Australia Section** forms IEEE WIE affinity group.
- Student branch formed at the **Chittagong University of Engineering and Technology, Bangladesh.**
- Student branch formed at the **Royal University of Bhutan, Thimphu.**
- **Chengdu (China) Section** forms IEEE Power & Energy Society chapter.
- Student branch formed at the **North China University of Technology, Beijing.**
- Student branch at **Southeast University, Nanjing, China,** forms IEEE Instrumentation and Measurement Society chapter.
- **Shanghai Section** forms IEEE Industry Applications Society chapter.
- **Xian (China) Section** forms IEEE Reliability Society chapter.
- Student branch at the **Hong Kong University of Science and Technology, Clear Water Bay,** forms IEEE Solid-State Circuits Society chapter.
- Student branches in India at **ABES Engineering College, Christu Jyothi Institute of Technology and Science, ITS Engineering College,** and **Kakatiya University College of Engineering** form IEEE WIE affinity groups.
- Student branch formed at **Diponegoro University, Semarang, Indonesia.**
- **Kansai (Japan) Section** forms IEEE WIE affinity group.
- Student branch at **INTI International University, Nilai, Malaysia,** forms IEEE Computer and Communications Society chapters.
- **Lahore (Pakistan) Section** forms IEEE Power & Energy Society chapter.
- **Philippines Section** forms IEEE Solid-State Circuits Society chapter.
- **Thailand Section** forms IEEE Broadcast Technology Society chapter.

SEND US YOUR NEWS The Institute *publishes announcements of new groups once they've been approved by IEEE Member and Geographic Activities. To send us local news, like student branch events and competitions, WIE or preuniversity outreach efforts, or other IEEE group activities, use our form on the Region News page at http://theinstitute.ieee.org/region-news.*

THE INSTITUTE ***(ISSN 1050-1797)*** *is published quarterly by The Institute of Electrical and Electronics Engineers Inc., 3 Park Ave., 17th Floor, New York, NY 10016-5997; tel. +1 212 419 7900. Periodicals postage paid at New York, NY, and at additional mailing offices. Canadian GST# 125634188. Annual subscription rate: US $26.95. Eight additional monthly issues are available online. The editorial policies for IEEE's major publications are determined by the IEEE Board of Directors. Unless otherwise specified, IEEE neither endorses nor sanctions any positions or actions espoused in* THE INSTITUTE. *Major IEEE boards review items within their purview prior to publication. When published in* THE INSTITUTE, *individual viewpoints of elected IEEE officers are labeled as such. They are reviewed by the individuals to whom they are attributed, unless they are a matter of record. The editorial staff is responsible for selection of subject matter and its placement within the issue.* ***POSTMASTER:*** *Send address changes to* THE INSTITUTE, *IEEE Operations Center, Coding Department, 445 Hoes Lane, Piscataway, NJ 08854. IEEE prohibits discrimination, harassment, and bullying. For more information, visit http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html.*

ISTOCKPHOTO (2)

SPECIAL REPORT:
CYBERSECURITY

IN LIGHT of recent highly publicized data breaches, denial-of-service attacks, and software vulnerabilities, the subject of cybersecurity—the focus of this special report—is particularly timely. The attacks showed that every organization's computers and data are at risk, no matter what its goals are or where it's located. The incidents have led to a renewed focus on improving the security and privacy of computers and networks.

HACKERS TAKE advantage of weak spots to break into systems that aren't properly patched or updated. Cybercriminals may download attachments containing malware or viruses or take advantage of computers that were disposed of without having been wiped clean. They can also gain access through vulnerabilities introduced by engineers and software designers. Often, software engineers lack the training and tools needed to mitigate and defend against security and privacy threats.

This report describes IEEE's efforts to make developers more knowledgeable through its Cybersecurity Initiative, launched in January 2014 by the IEEE Computer Society and the IEEE Future Directions Committee, the organization's R&D arm. The initiative is working to educate engineers and others and is developing tools to help prevent software design flaws that could compromise privacy and security.

The issue also deals with meeting the challenge of protecting private information on mobile devices [see p. 8] and what must be done so that cybersecurity is taken more seriously as a profession [p. 9]. And we've profiled Greg Shannon, chair of the IEEE Cybersecurity Initiative [p. 14].

The initiative also aims to get the word out about IEEE's expertise in cybersecurity. The organization has been offering products, conferences, and standards on the subject for more than three decades [p. 12].

This issue also announces the winners of the 2014 IEEE election and includes the list of senior members elevated to the 2015 class of Fellows, as well as proposed revisions to the IEEE constitution that members will be asked to vote on this year.

—Kathy Pretz, Editor in Chief

Protecting Against Cyberattacks

IEEE is working to help engineers fortify systems BY KATHY PRETZ

IN THE FACE of growing computer security breaches, it makes little sense to be cavalier about cybersecurity and cyberprivacy. Just ask the European Central Bank, Korea's Hydro and Nuclear Power Co., Microsoft, or Sony Pictures—some of the recent cyberattack victims. Credit-card payment systems have been raided. Floor plans of sensitive facilities have been posted on social media. Gaming services have been disrupted and employees' personal information leaked. Companies' reputations have been damaged, customers have fled, top executives have been fired, and hefty fines incurred.

What's more, the financial impact of an intrusion is growing. Last year, the average cost per incident increased 15 percent over 2013 to US $3.5 million, according to the annual Cost of Data Breach Study sponsored by IBM and conducted by the Ponemon Institute, of Traverse City, Mich. The study surveyed 250 companies in 11 countries and found that the cost incurred for each lost or stolen record containing sensitive information increased more than 9 percent compared with the previous year, to $145.

Attackers gain access in many ways, including through viruses and malware, stolen passwords, and personal information stored on publicly accessible directories. As has been the case for decades, hackers find their way in because of engineering and operating mistakes. The IEEE Cybersecurity Initiative wants to change that.

"It has become clear that, generally, engineers have not had sufficient training nor been encouraged to have a mind-set that considers how an adversary might thwart their system, whether it's on the security side, the privacy side, or the vulnerability side," says the initiative's chair, IEEE Senior Member Greg Shannon. He's chief scientist for the CERT Division at the Carnegie Mellon University Software Engineering Institute, in Pittsburgh. The initiative was established in January 2014 by the IEEE Computer Society and the IEEE Future Directions Committee.

Not enough investment is being made to ensure that sufficient security and privacy controls are implemented, Shannon says, adding that the R&D community has not given engineers the tools they need to understand all the possible threats against their systems and how to mitigate them.

The initiative is accelerating innovative research and developing cybersecurity privacy technologies to protect commerce, innovation, and freedom of expression.

"Now is the time not only for better defensive measures but also for cybersecurity standards and best practices that consider the entire technology life cycle," Shannon says. "It is IEEE's responsibility to emphasize strongly the things that can improve security and privacy, and this means not ignoring the engineering mistakes made in developing and operating software systems. These may be less noticeable but can prove just as harmful.

"Alone of any professional society, IEEE has been involved in cybersecurity from soup to nuts," he adds.

IEEE has been helping engineers recognize, resist, and recover from cyberattacks for more than three decades. The annual IEEE Symposium on Security and Privacy, for example, marked its 35th anniversary last year. And IEEE

offers conferences, publications, standards, and other services [see p. 12]. But many in the cybersecurity field are unaware of the breadth, depth, and longevity of IEEE's work, according to Shannon. The initiative plans to change that, too, along with adding new offerings to the field.

SECURITY: FRONT AND CENTER

About half of all security breaches are possible because of flaws in the software's architecture and design. The rest result from bugs in the software's implementation—the overall design may appear sound, but some aspect of its execution fails. The security industry has been focused mostly on finding and eradicating bugs; it has virtually ignored the fact that design flaws may also be the subject of attack. Unfortunately, not much reference material exists on how to avoid these types of flaws.

That's why the initiative established the IEEE Center for Secure Design, hosted on the initiative's website at http://cybersecurity.ieee.org/center-for-secure-design.html. It focuses on identifying and preventing software design flaws. The center was formed by such organizations as Athens University of Economics and Business, Cigital, EMC, Google, Harvard, Twitter, and the University of Washington, Seattle. The CSD released a report in August detailing the top 10 most widely and frequently occurring software security design flaws, as well as recommendations for avoiding them. The report is also on the initiative's website.

GUARDING MEDICAL DATA

Wearables, smartphone apps, portable diagnostic units, and other personal health-monitoring devices are gaining in popularity. More gadgets are sharing health and medical information electronically, which puts the privacy and security of the data at risk.

"People don't want just anybody to be able to access their health profile and related information," Shannon points out.

"Because these devices are in low-power, low-bandwidth environments, they present challenges from an engineering point of view," he says. The hurdles include ensuring that data from wearable trackers are being uploaded to an authorized device and the platform uploading the data is getting it from the correct sensor. "A solution to this challenge that works on the desktop might not work for a wearable device," Shannon adds.

And larger medical devices come with their own set of security concerns. The medical community has generally been unconcerned about the possible theft or manipulation of its data because medical devices have traditionally been ensconced in hospitals and medical facilities. But once the machines become portable and common in homes and their information is increasingly shared, the data could be manipulated in ways the original engineers never considered, Shannon cautions.

"Many of these devices use vulnerable components and operating systems, and patching them is a concern," he says. "Engineers have to be very careful about whether the patched product will still be certified by agencies that oversee them, like the U.S. Food and Drug Administration, and whether the update causes something else to malfunction. If it's your pacemaker, you care a great deal about that."

To that end, the initiative is developing "building codes" for medical devices similar to those used in the construction industry.

"Security and privacy issues—what is important and what is reasonable or what is not—are still being defined by society," Shannon says. "Part of a broader aspect of the initiative is to help understand the decisions that must be made, as well as larger issues such as who has a right to what data, and what can and can't companies be allowed to do with personal data. We know that IEEE will help inform that conversation." ◆

BONNIE NANI (2)

Mobile Devices Lack Security

It's a problem developers can no longer ignore

BY MONICA ROZENFELD

OF THE WORLD'S 7 billion people, 6 billion rely on mobile phones or tablets to bank, shop, post to social media, and monitor their health. With all the personal and professional information being shared, it's important that data from mobile devices be secure. Yet that's rarely the case.

Securing such information is no small feat. Unlike applications designed for laptop and desktop computers—often created by just a handful of companies—there are now more than 1 million apps for smartphones and tablets designed by nearly the same number of developers. Many of them are novice designers with little concern for protecting the security and privacy of the data their apps collect and store. Moreover, when downloaded, many of the apps have access to other information in the mobile device, making them potential outlets for data leakage and theft.

That's just one issue. Another is malicious websites. More than half of websites are live for 24 hours or less, which makes them difficult to monitor for harmful content. Malware—short for *malicious software*—is used to gather sensitive information, gain access to private networks or accounts, or disrupt system operations. Consumers unknowingly encountering malware can give hackers entry into their mobile devices.

Unlike the sophisticated scans that run on desktop systems, mobile devices have limited options for running antimalware or antivirus software; the gadgets don't have the computing and battery power to handle the workload.

"The threats to mobile devices are part of an enormous problem," says Greg Clark, CEO of Blue Coat Systems, an information security company in Sunnyvale, Calif. "Many users don't fully grasp the scope of the efforts contrived to entice them to download malware on their devices."

Blue Coat issued a report last year on mobile threats, covering some of the concerns above. Clark looks at security in mobile devices as akin to walking through one of the most dangerous neighborhoods wearing an expensive suit and carrying a fancy briefcase. "Some of these mobile devices are roaming through some of the worst, yet most advanced, security-threat spaces in the world," he says. "These devices are hardly protected."

Developers could choose, however, to make mobile devices more resistant to attacks, Clark says.

A NEW FRAMEWORK

Methods for increasing security in operating systems have changed dramatically over the years. "It's been a cat-and-mouse game," Clark explains. "Security companies like ours find a way to stop hackers, who then find another way in."

Clark and Qing Li, Blue Coat's chief scientist, are developing a framework they call an infrastructure-centric security ecosystem with a cloud defense, which mobile developers could adopt for their operating systems. They describe it in an article, "Mobile Security: A Look Ahead," published in *IEEE Security & Privacy* magazine.

Their cloud-based framework would be an agile system able to keep pace with evolving threats. The framework would consist of application proxies, real-time content categorization and rating engines, and real-time URL analysis engines to help decide which websites are safe to browse. The Blue Coat model would also filter malware from compromised websites to prevent an attack from ever reaching a user's device.

Furthermore, the framework would help prevent data leaks by relying on engines designed to block potential breaches that can give hackers access to passwords, online accounts, documents, and more. The cloud feature would make it possible to collect information gathered from all the devices connected with the framework to more easily identify new malicious applications and Web-based threats.

> *Mobile devices are roaming through some of the worst, yet most advanced, security-threat spaces in the world.*

Antivirus and antimalware engines accessible through a cloud-based service would take the load off the devices, Li says. As part of the scanning service, the network could catalog and report on the reputation, risk, and vulnerability levels of each installed application—which would help users decide what apps to keep.

Network-based inspections are scalable, flexible, and able to intercept and disrupt threats, Clark says. "In the Wild West of mobile apps and the rapid sprouting of websites," he says, "users want their networks to inform them when they are accessing malicious content and proactively terminate the attacking threats. And we want to allow the network to be programmable to offer layered defense for the end points."

The willingness to have an open network, however, has to come from the users and service providers in order to allow security solutions to inspect and analyze activities to ensure harmful content is not being accessed, Li says. "Mobile security," he points out, "requires an entire ecosystem to participate in the defense of mobile devices and their users." ◆

ISTOCKPHOTO

Raising the Bar for Cybersecurity Specialists

More training and standards are needed to meet the growing demand BY JOHN R. PLATT

DO YOU KNOW how to become a cybersecurity professional? Do you know what courses to take, which certifications are needed, and what skills employers require? As a hiring manager, can you assess whether your new hire knows how to write secure mobile apps, defend systems against cyberattacks, or protect customer credit-card data?

The truth is, not many people can answer those questions. And that uncertainty, experts say, is a problem for the cybersecurity industry. Its rapid growth during the past decade has led to an unclear educational path for students. There is also an absence of generally accepted qualifications that tell hiring managers and human resources departments which job candidates have the right experience and credentials.

"This confusion causes the profession to grow less efficiently than it could," says IEEE Senior Member Greg Shannon, chief scientist for the CERT Division at Carnegie Mellon University Software Engineering Institute, in Pittsburgh, and chair of the IEEE Cybersecurity Initiative. "People can't say, 'These are the credentials I need' and 'This is how much it is going to cost me to get them.'"

The lack of clarity, Shannon says, has contributed to a widespread shortage of trained, experienced cybersecurity professionals. Similarly, it has created a challenge for employers to hire people with the right skills. HR reps find themselves confronted with a variety of certifications from about two dozen organizations.

"There are people out there who are being positioned, rightly or wrongly, beyond their skills to address cybersecurity," Shannon says. "Meanwhile, not enough new people are entering the profession to fill the void."

LET'S SET STANDARDS

To bridge the gap, researchers from the Pell Center at Salve Regina University, in Newport, R.I., are calling on the cybersecurity industry to create professional standards for those in the field. In July, they issued "Professionalizing Cybersecurity," a report that calls for an overarching professional association to create clear paths for a variety of careers.

"What we propose is not just a way to put more people in the pipeline," says Pell Fellow Francesca Spidalieri, who coauthored the report with Lt. Col. Sean Kern, a Pell Center adjunct fellow with the U.S. Air Force. "It is also about guaranteeing that those in the industry reach the highest professional standards."

The industry has tried to respond to the needs of the marketplace by developing certifications and other educational standards for various career paths. However, these have sprung up individually. They often overlap each other and leave gaps.

The report found that cybersecurity is composed of 31 different specialties dealing with such areas as information assurance compliance, systems security architecture, and digital forensics. These specialties are served by at least 23 different certification programs from such organizations as the American Society for Industrial Security, the Computer Security Institute, and the International Society for Professionals in E-Commerce. Plus, the field is rife with conflicting definitions and competing requirements.

Universities should establish a more unified educational path for students interested in a cybersecurity career, Kern says, noting, "There are no nationally or internationally accredited programs that universities can adhere to and publicize in a way that a student can say, 'That's where I can obtain the kind of education I need to get started in the cybersecurity profession.'"

LEARNING THE LANGUAGE

The Pell report offers recommendations for developing a more organized cybersecurity profession, including establishing clear bodies of knowledge and educational paths for the 31 workforce specialties.

"You really have to have that body of knowledge, along with some means of assessing if a person understands that knowledge and can apply it creatively against whatever problems an organization faces," Spidalieri says. "That's the language of a profession."

There are many different roles to fill in cybersecurity, says IEEE Senior Member Gary McGraw, chief technology officer of Cigital—a software security firm in Dulles, Va.—and a volunteer for the IEEE Cybersecurity Initiative.

"Each role needs to have its own education and experience path," McGraw says. "If you think of security like medicine, you need first responders, nurses, doctors, brain surgeons, and everything in between."

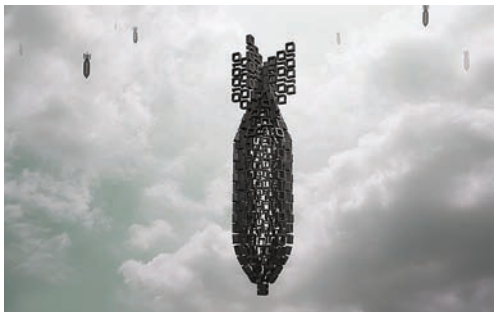
The largest cybersecurity certification program, the Certified Information Systems Security Professional (CISSP), would serve the emergency medical responders, nurses, and maybe doctors, but it wouldn't help the brain surgeons and other specialists, McGraw says.

"Organizing a common body of knowledge in any area is always useful," he says. "A CISSP certification guarantees only that you have a modicum of knowledge about a swath of cybersecurity. Your knowledge may be wide but not very deep."

Spidalieri and Kern also call for each specialty to develop its own code of ethics, something currently lacking. "Part of what we learn in engineering these systems correctly is how to break in," McGraw says. "You need to break into systems and find security flaws before hackers do." Otherwise, he points out, some will use those same skills for nefarious purposes. ◆

ERIK ISAKSON/GETTY IMAGES

OPINIONS



QUESTION OF THE MONTH

Should We Fear a Catastrophic Cyberattack?

In a survey by the Pew Research Center of 1,642 cybersecurity experts, 61 percent said a widespread cyberattack will occur in the next 10 years, leading to at least one of the following: the theft of tens of billions of dollars, harm to a nation's security and capacity to defend itself, or a significant loss of life.

CHIME IN *Tell us what you think by commenting online at http://theinstitute.ieee.org/opinions/question.*

Sparking Conversation

In December, *The Institute* delved into software-defined networks (SDNs), which decouple hardware from software and then execute the software either in the cloud or in clusters of distributed IT servers. Online, we blogged about famously false technology predictions and published a tribute to the late Ralph Baer, the father of video games. The conversation continued on our website.

ASK THE EXPERTS

Antonio Manzalini, chair of the IEEE Software Defined Networks Initiative, and Prosper Chemouil, chair of the initiative's conference subcommittee, answered readers' questions about SDNs.

Q: ***How will SDNs hold up in the face of massive congestion?***
Manzalini: Traffic engineering and the orchestration of functionalities will help lessen the risk of massive congestion. In SDNs, data and control planes could be logically and physically decoupled, easing any congestion.

Q: ***What security issues are associated with SDNs?***
Chemouil: The risk is that a centralized SDN controller could be a single point of attack or failure. To get around this, some researchers have proposed setting up multiple SDN controllers, either in a distributed or hierarchical structure.

Q: ***How will SDNs facilitate the Internet of Things?***
Manzalini: SDNs and network functions virtualization (NFV) are accelerating the transition to telecommunications infrastructure with more pervasive and embedded processing and storage capabilities.

SDNs will become "nervous systems" for things like terminals, drones, robots, machines, and cars. With SDNs and NFV, the border between the telecom infrastructure and what connects to the "things" will blur.

HACKERS FOR HIRE

We asked readers whether tech companies should hire hackers to find security flaws in their software.

"Professional hackers are specialists, hence best qualified to find and fix security problems, but how do you know they didn't install or leave open a 'back door'?"

"No, just as banks shouldn't hire thieves as security guards."

"The FBI and some casinos in Las Vegas have hired former criminals to work for them. Obviously, this is potentially risky, but in some cases it could be effective. There's no simple black-and-white answer here."

FALSE PREDICTIONS ABOUT TECH

Readers added to our list of famous predictions that proved to be wrong.

"Television won't be able to hold on to any market it captures after the first six months. People will soon get tired of staring at a plywood box every night." *—Darryl F. Zanuck, executive at 20th Century Fox, in 1946*

"Two years from now, spam will be solved." *—Bill Gates, in a 2004* Information Week *article*

REMEMBERING RALPH BAER

Tributes poured in for the IEEE Fellow and inventor of the first video game console, who died on 6 December.

"This man paved the way for innovative human-computer interaction and interfaces. It's amazing to think that it all started with his putting pen to paper at a bus terminal."

"I had the pleasure of hearing Ralph Baer as the keynote speaker at an IEEE New Hampshire Section annual meeting. Prior to that, I had no idea that video games had started in this state."

"Many people have been unable to find work they love doing, perhaps because they've been taught there can be no gain without pain. This man obviously loved what he did. *Ave atque vale.*" [Latin for "Hail and farewell."] ◆

HIROSHI WATANABE/GETTY IMAGES

IEEE QUICK GUIDE

THE IEEE SUPPORT CENTER

Visit https://supportcenter.ieee.org to search the knowledge base for information by topic, read answers to frequently asked questions, submit your own question, or initiate an online chat with an agent.

THE IEEE CONTACT CENTER

For assistance with IEEE products and services or help with publication delivery

FOR E-MAIL INQUIRIES
The IEEE Contact Center is open from 4:30 p.m. ET (20:30 GMT) Sunday to 4:30 p.m. ET Friday.
E-mail: contactcenter@ieee.org

Tel.: +1 732 981 0060 (worldwide)
Tel.: +1 800 678 4333 (U.S. and Canada)
Fax: +1 732 562 6380

TO RENEW MEMBERSHIP
http://www.ieee.org/renew

TO JOIN
http://www.ieee.org/join

CONTACT POINTS

IEEE OPERATIONS CENTER
Tel.: +1 732 981 0060
445 Hoes Lane
Piscataway, NJ 08854-4141 USA
Business hours: 8 a.m. to 5 p.m. ET (12:00 to 21:00 GMT), Monday through Friday

IEEE CORPORATE OFFICE
New York City
Tel.: +1 212 419 7900

IEEE–USA
Washington, D.C.
Tel.: +1 202 785 0017
Fax: +1 202 785 0835
E-mail: ieeeusa@ieee.org

ASK*IEEE DOCUMENT DELIVERY
Tel.: +1 800 949 4333
Fax: +1 303 758 1138
E-mail: askieee@ieee.org

CONFERENCE INFORMATION
Tel.: +1 732 562 3878
Fax: +1 732 981 1769

ELEVATION FORMS
Associate to member:
http://ewh.ieee.org/forms/v2/md/memelv.htm
Member to senior member:
http://www.ieee.org/membership_services/membership/senior/application/index.html

IEEE MEMBER DISCOUNTS PROGRAM
Tel.: +1 800 438 4333
Fax: +1 732 981 0538
E-mail: discounts@ieee.org

OMBUDSMAN
Tel.: +1 800 678 4333
E-mail: ombudsman@ieee.org

SECTION AND CHAPTER INFORMATION
Tel.: +1 732 562 5511
Fax: +1 732 463 9359
E-mail: sec-chap-support@ieee.org

STUDENT ACTIVITIES INFORMATION
Tel.: +1 732 562 5527
Fax: +1 732 463 3657
E-mail: student-services@ieee.org

TECHNICAL SOCIETIES INFORMATION
Tel.: +1 732 562 3900
E-mail: society-info@ieee.org

the institute

EDITOR IN CHIEF
Kathy Pretz, k.pretz@ieee.org

ASSOCIATE EDITOR
Monica Rozenfeld, m.rozenfeld@ieee.org

SENIOR EDITORIAL ASSISTANT
Amanda Davis, amanda.davis@ieee.org

EDITORIAL CONSULTANT
Alfred Rosenblatt

COPY EDITORS
Joseph N. Levine, Michele Kogon, Mark Yawdoszyn, Peter Borten

SENIOR ART DIRECTOR
Mark Montgomery

ART DIRECTOR
Bonnie Nani

PHOTOGRAPHY DIRECTOR
Randi Silberman Klett

DIRECTOR OF PERIODICAL PRODUCTION SERVICES
Peter Tuohy

EDITORIAL & WEB PRODUCTION MANAGER
Roy Carubia

WEB PRODUCTION COORDINATOR
Jacqueline L. Parker

MULTIMEDIA PRODUCTION SPECIALIST
Michael Spector

EDITORIAL OFFICES
IEEE Operations Center
445 Hoes Lane, Piscataway, NJ
08854-4141 USA
Telephone: +1 732 562 6825
Fax: +1 732 562 1746
E-mail: institute@ieee.org
Web: theinstitute.ieee.org

IEEE MEDIA

PUBLISHER
James A. Vick

ADVERTISING SALES COORDINATOR
Mindy Belfer

BUSINESS MANAGER
Robert T. Ross

MARKETING & PROMOTION MANAGER
Blanche McGurr

ADVERTISING SALES
+1 732 562 3946

ADVERTISING PRODUCTION MANAGER
Felicia Spagnoli

ADVERTISING PRODUCTION
+1 732 562 6334

Printed with inks containing soy and/or vegetable oils

SUSTAINABLE FORESTRY INITIATIVE
Certified Chain of Custody
Promoting Sustainable Forestry

HOWARD E. MICHEL IEEE PRESIDENT AND CEO

Toward a More Secure Future

DARREN CARROLL

HISTORY IS littered with companies that did almost everything right but failed anyway. Some failed because they didn't understand what their business was, or should have been. For example, Eastman Kodak thought it was in the film business. Actually, it was in the business of capturing and preserving images. It ignored disruptive innovations that would render its traditional film business obsolete. Today, it is far from the powerhouse company it once was.

In 1975, Steven Sasson, an electrical engineer on Kodak's research team, created the first digital camera—decades before digital cameras flooded the market and built-in cameras became commonplace in cellphones. The company saw no business opportunity for its digital camera, because it could not imagine a world in which its film was supplanted by digital media. Less than 30 years later, Kodak was struggling to reinvent itself in the digital media world. Film had become an anachronism.

OUTSIDE THAT BOX

Like Kodak, IEEE cannot allow itself to continue thinking within its traditional parameters. Members and volunteers come together to create, disseminate, and use information to advance technology for humanity. But we are much more than a membership organization, conference organizer, publisher, and standards developer.

Our world is increasingly driven by information. Yet we talk about papers—whether presented at a conference or archived in a journal—as if the *papers* were the information. Papers are a centuries-old technology to record and share information. They were born in a time when scholars collaborated through letters delivered on horseback. This is the 21st century. We need a new medium for sharing our information.

We hold more than 1,400 conferences annually, face-to-face meetings that are episodic. Nothing new here; people have been holding meetings for eons. And between meetings, people are communicating and innovating 24/7/365, across the globe. Some are using video chat tools, webinars, and blogs. Episodic, face-to-face meetings are becoming obsolete in the Internet Age.

In the future, nearly all scholarly and business information will be created by individuals who never meet in person—brought together through technology and bound by a passion to better the world. Information will be consumed by yet another set of individuals, indifferent to its source, working on problems spanning diverse disciplines. Time will be critical, whether to save lives or to maintain competitive advantage in the marketplace.

More than ever, IEEE needs to address the future of information.

More than ever, IEEE needs to address the future of information: how technical professionals will create it, share it, and use it in an evolving, global marketplace. Imagining and acting on that future are critical to IEEE's continued success.

We've taken a lot of positive steps to build this future. Articles in our IEEE Xplore Digital Library have been transformed from static PDF files into interactive XML. We've built technical communities spanning societies to better assist researchers working on multidisciplinary problems.

To this end, we ran a pilot program in 2014, and this year we'll be launching IEEE Collabratec. It will provide a suite of online tools with which to network, collaborate, and create—making publishing faster and easier.

However, we are not alone. Facebook, LinkedIn, ResearchGate, Twitter, and Wikipedia, to name a few, are also innovating in the information space. While they are not our direct competitors today, they could be if we miss the sea change in how technologists produce, acquire, and use information.

LOOKING AHEAD

IEEE is focusing this year on not just our immediate future but also on what is coming in 5, 10, and 15 years. We will talk about the future of information, the future of conferences, the future of membership in professional technical organizations, the future of publications, and the future of standards development. In short, we will talk about the future of IEEE.

IEEE's Board of Directors has already been incorporating these strategic discussions into the fabric of our meetings. Such a strategic examination and visualization of IEEE's future is an absolute necessity. It is being given priority at every board meeting.

For IEEE to remain a touchstone organization for engineers and technologists, it must evolve. That evolution, while swift, cannot be haphazard. Instead, there must be a comprehensive vision of what IEEE is as a community today and what we wish to be in the future.

By the end of this year, it is my goal to have an actionable vision, articulated in a comprehensive strategic plan and accompanying global strategy plan everyone in our community can embrace. But most important, I want that vision to be an outgrowth of the ideas and insights gathered from across IEEE.

I look forward to your thoughts and suggestions. Please send them to me at president@ieee.org. ◆

Help With Fending Off Cyberattacks

The resources needed to combat computer-security threats BY KATHY PRETZ

IEEE OFFERS a variety of tools and services to help make systems more secure.

WEB PORTAL

Cybersecurity.ieee.org houses the latest activities of the IEEE Cybersecurity Initiative, including its Center for Secure Design, which seeks to identify common software design flaws. The portal also has links to organizations involved with protecting computer security and privacy, as well as excerpts from books on software security and articles from the IEEE Computer Society Digital Library.

PODCASTS

The portal also has a link to the entire catalog—more than 100 episodes—of the "Silver Bullet" podcast, which IEEE Senior Member Gary McGraw has been hosting for more than eight years. McGraw, chief technology officer at the software security consultant Cigital, interviews security experts on a variety of topics.

One of the episodes, for example, is a roundtable discussion with people who helped establish the Center for Secure Design. They discuss its origin, explain why design flaws are more difficult to fix than implementation bugs, and point out the problems with software designed for cars.

PUBLICATIONS

IEEE Security & Privacy magazine, from the IEEE Computer Society, publishes articles by leaders in the field. It covers diverse aspects of information assurance such as legal issues, privacy concerns, tools for securing information, attack analysis, cybersecurity design trends, and developments in hardware and software.

Also from the Computer Society is the bimonthly *IEEE Transactions on Dependable and Secure Computing*, which publishes archival research results focusing on the foundations, methodologies, and mechanisms of systems and networks. Articles focus on measurement, modeling, and simulation techniques, as well as on foundations for jointly evaluating, verifying, and designing within performance, security, and dependability constraints.

IEEE Transactions on Information Forensics and Security, published by the IEEE Signal Processing Society, covers the science, technologies, systems, and applications related to information security, biometrics, surveillance, and related fields.

Other IEEE publications that cover security regularly include *Computer*, *IEEE Pervasive Computing*, *IEEE Software*, *IEEE Transactions on Reliability*, and *IT Pro*.

Look for them in the IEEE Xplore Digital Library.

EDUCATIONAL COURSES

The Computer Society offers four software security–related courses: Foundations of Software Security, Secure Software Design, Managing Security Software Development, and Security Software Coding. The foundations course, for example, provides an overview of countermeasures used to thwart well-known and emerging threats. The course on coding presents language- and application-specific techniques. Each course takes about 7 hours.

They can be found in the Professional Education section of the society's website.

SUPPORT SERVICES

The IEEE Industry Connections Security Group is composed of organizations that pool their resources to address threats. The ICSG was established in 2009 under the umbrella of the IEEE Standards Association's Industry Connections program, which brings together market competitors to build consensus and incubate standards, products, and services suitable for sharing.

Four subgroups have been established. The Malware Working Group tackles malicious software that can infiltrate operating systems and cause all kinds of trouble, including the loss of personal data. The group is establishing better ways of sharing malware samples and the information associated with them, so as to improve computer security. In 2010, the ICSG released free XML schemes for sharing malware samples.

The Malware Metadata Exchange Format Working Group also focuses on expanding the breadth of information exchanged.

The Privilege Management Protocols Working Group develops procedures for efficient authentication and secure determination of "who can do what." The "who" is defined as a framework that uses public key–based identities for authentication.

In cryptography, a public key is a value provided by a designated authority that, combined with a private key derived from the public key, can be used to encrypt messages and digital signatures. The authorization of "what" a device can do is based on management of the identity that can be authenticated, formed by hashing the public key. This approach has considerable advantages over shared key–based systems.

The IEEE Standards Association offers other types of assistance to combat malware. The IEEE Anti-Malware Support Service has two tools: the Clean File Metadata Exchange (CMX) and a "taggant" system.

The CMX provides real-time access to information related to clean software files, even prior to the publication of the corresponding software. That can help reduce the number of false positives detected by antivirus software as it searches for malware.

The taggant system places a cryptographically secure marker in files created by commercial software distribution packaging programs, or packers. Legitimate packers often are abused by malware creators that develop many difficult-to-detect variants of their malware. The taggant system's markers identify the specific packer user's license key, enabling a blacklisting of the malware. The system also reports suspicious files.

Information about all the Standards Association services is available at http://www.standards.ieee.org. ◆

IEEE Standards on Cybersecurity

They cover a variety of applications, including authentication and data protection BY MONICA ROZENFELD

THE IEEE STANDARDS Association has introduced a number of standards related to cybersecurity, with more in the works.

■ IEEE 1888.3-2013

APPROVED OCTOBER 2013

"IEEE Standard for Ubiquitous Green Community Control Network: Security" supports enhanced security management functions for sustainable computing. Included are security requirements, system security architecture definitions, and a description of authentication and authorization. The standard helps avoid unintended data disclosures to the public and unauthorized access to resources.

■ IEEE 1686-2013

APPROVED JANUARY 2013

"IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities" defines the functions and features to be integrated into intelligent electronic devices for critical infrastructure protection programs. Access, operation, configuration, firmware revision, and data retrieval are addressed.

The following are under development.

■ IEEE P1711

"IEEE Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links" specifies a practice that can protect the integrity and confidentiality of communications over phone lines, radio waves, fiber optics, and more. The protocol could be implemented in new equipment or when retrofitting existing systems.

■ IEEE P2030.102.1

"IEEE Standard for Interoperability of Internet Protocol Security (IPsec) Utilized Within Utility Control Systems" promotes in four basic steps the security of control systems deployed by electric utilities: defining functional requirements based on needs, selecting open-source specifications to meet those requirements, developing interoperable configuration profiles for the specifications, and testing and validating the configurations.

The proposed standard would allow for functionality to be applied at the device level on a case-by-case basis. It offers guidelines that would make it easier for utilities to procure and implement secure systems, provide adequate security controls, and minimize efforts to configure devices that support cybersecurity functions.

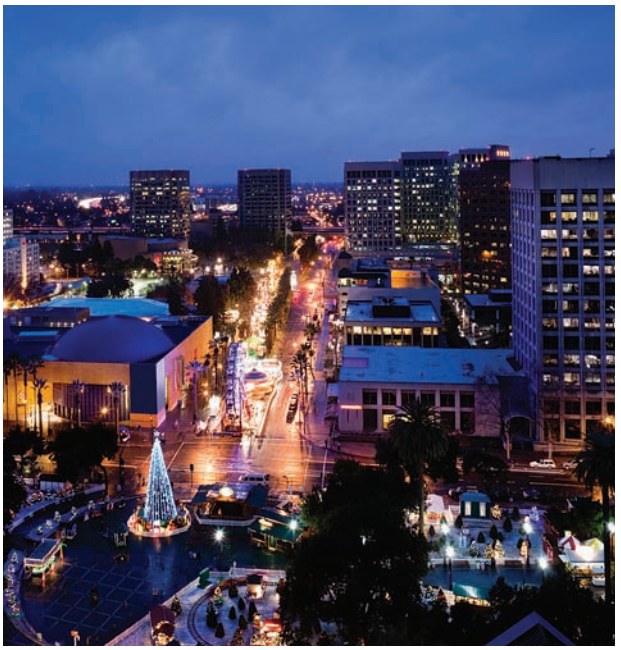
■ IEEE P802.1AEcg

"IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security Amendment: Ethernet Data Encryption Devices" facilitates secure communication over publicly accessible networks for which security has not already been defined. ◆

WALTER BIBIKOW/GETTY IMAGES

Cybersecurity Conferences

Upcoming IEEE events will address identity protection, malware, and trust protocols



IEEE Symposium on Security and Privacy

SAN JOSE, CALIF.; 18–20 MAY

TOPICS: Access control, accountability, application security, cyberattacks and defenses, authentication, cloud security, forensics, intrusion detection, malware, mobile privacy and security, security architectures, privacy policies, Web security and privacy, and embedded and distributed systems.

SPONSOR: IEEE Computer Society
VISIT: http://www.ieee-security.org/TC/SP2015

■ IEEE International Symposium on Technologies for Homeland Security

WALTHAM, MASS.; 14–16 APRIL

TOPICS: Cybersecurity, biometrics and forensics, land and maritime border security, cyberattack and disaster preparation, cloud computing, big data, personnel screening, secure information sharing, supply chain monitoring and defense, telecommunications security, and system and network recovery.
SPONSOR: IEEE-USA
VISIT: http://ieee-hst.org

■ IEEE International Symposium on Hardware-Oriented Security and Trust

MCLEAN, VA.; 5–7 MAY

TOPICS: Cyberattacks and detection techniques, hardware-based security, trust protocols, trusted information flow, remote enabling and disabling techniques for integrated circuits, intellectual property and watermarking, hardware metering, supply chain risk mitigation, and secure remote sensing.
SPONSOR: IEEE Computer Society
VISIT: http://www.hostsymposium.org

■ IEEE International Conference on Trust, Security, and Privacy in Computing and Communications

HELSINKI; 20–22 AUGUST

TOPICS: Network computing, operating systems, software and applications, social networks, e-commerce, mobile and wireless communications, Web applications, parallel and distributed systems, and cloud computing.
SPONSOR: IEEE Computer Society
VISIT: https://research.comnet.aalto.fi/Trustcom2015

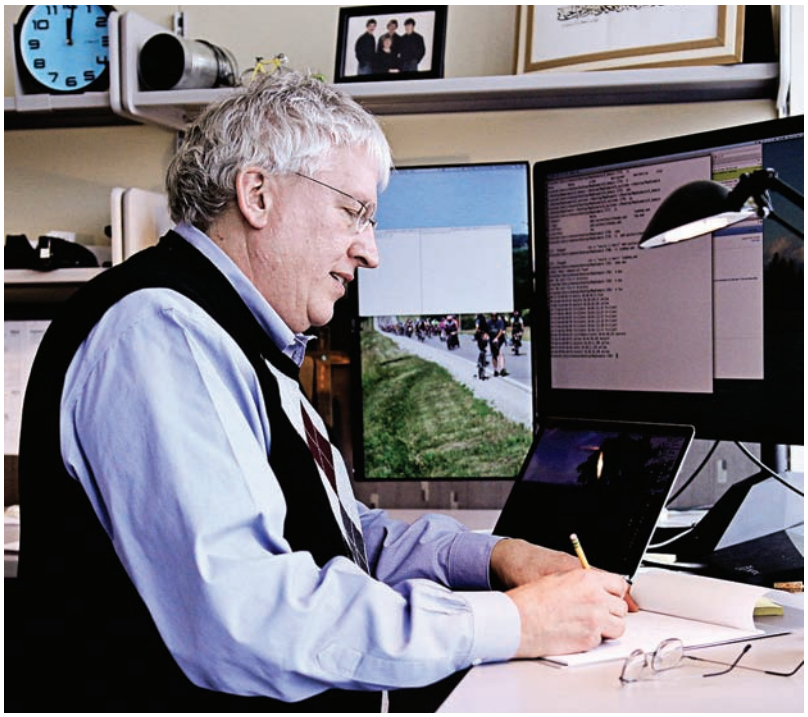
■ IEEE Conference on Communications and Network Security

FLORENCE, ITALY; 28–30 SEPTEMBER

TOPICS: Privacy and anonymity, biometric authentication and identity management, computer and network forensics, data and application security, data protection, location security, outsourcing of network and data communications services, traffic analysis, and intrusion detection and prevention.
SPONSOR: IEEE Communications Society
VISIT: http://cns2015.ieee-cns.org ◆

Greg Shannon: Cybersecurity Champion

Safeguarding computer systems from serious threats BY **PRACHI PATEL**



DAVID BIBER/CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE

IN TODAY'S digital, data-reliant world, cyberthreats can take many forms, including hackers conducting cyberespionage, troublemakers hijacking electronic highway signs, and globe-spanning cybercrime rings perpetrating bank fraud.

IEEE Senior Member Greg Shannon's job is to help the United States stay at least one step ahead of increasingly sophisticated cybercriminals. He is chief scientist at CERT, part of the Carnegie Mellon University Software Engineering Institute, in Pittsburgh, which is funded by the U.S. Defense Department's R&D center. At CERT, he partners with government, academia, law enforcement, and industry to develop methods and tools to deal with cyberthreats.

In November, Shannon was named chair of the IEEE Cybersecurity Initiative. Launched in January 2014, its mission is to advance the field through education, conferences, and standards.

CERT was formed in 1988 to counter the Morris worm, the first computer worm distributed through the Internet. That incident "brought the Internet as it was then to its knees," notes Shannon, who joined the organization five years ago. "CERT was part of the response team to get it back online."

Responding to cybercrime by providing analytical support to federal law enforcement agencies remains an important part of CERT's mission, but the explosion of the Internet has far expanded its scope.

SAFETY IN LAYERS

Cybersecurity today involves much more than defensive measures, Shannon points out. It is vital for organizations to build secure foundations and anticipate security challenges. That includes designing secure code, finding software vulnerabilities, putting management structures in place to deal with risks, and identifying possible threats from inside a company.

Organizations regularly fail to incorporate strategies for reducing software vulnerability and risk, Shannon says. He intends to start changing that by delivering inexpensive, practical solutions to government agencies. CERT researchers have, for example, developed malware analysis tools and secure coding techniques that help software developers reduce glitches in their systems and find defects in applications. Although they are produced for government clients, many of the tools are available in open-source formats for the general community, Shannon says.

But even if organizations implement better strategies, no defined metrics exist for gauging software security. "If you can't measure something and provide feedback, then you can't help people improve their systems," Shannon says.

His research focuses on developing cybersecurity metrics and effective ways to analyze them. He says he expects to have useful metrics and measurement techniques in the next two years.

But building security into code from the get-go is safer and more economical than finding and fixing bugs later on, Shannon notes. He has led the development of secure coding guidelines for software that includes C and C++, Java, and the Android platform. Cisco, Oracle, and other companies have adopted CERT's guidelines.

Shannon is also trying to understand how organizations can integrate security technologies throughout the software development chain. "Today, developers can find a lot of open-source projects and tools and pull them together to create different technologies," he says. "But that compromises security and privacy."

The IEEE Cybersecurity Initiative gives Shannon an ideal platform for furthering his cybersecurity mission. He points to IEEE's important role in promoting security research, its substantial membership, and its position in the engineering community, as well as its "amazing" standards development program.

He also aspires to bring the security and privacy communities together. Too often, data security and privacy concerns are perceived as adversarial, he says, and he wants people to see that they are complementary.

A WINDING ROAD

Shannon earned a bachelor's degree in computer science from Iowa State University, in Ames, in 1982. For three of his undergraduate years, he worked at the school's Ames Laboratory, programming computers to analyze mass spectrometry data. That gave him a strong sense of the computer's role in science.

After earning his Ph.D. in computer science in 1988 from Purdue University, in West Lafayette, Ind., he became a professor of computer science at Indiana University in Bloomington.

He soon realized that teaching was not his calling, however, and he moved on to Los Alamos National Laboratory, in New Mexico, in 1993, to work on fraud detection and security. He left a year later to launch Spanning Tree, which developed technology for network scanning and vulnerability assessment. After a Canadian network company bought Spanning Tree, he joined Ascend Communications in Dublin, Ohio, as an engineering manager, working on firewalls and other security software.

Lucent Technologies acquired Ascend in 1999, and Shannon became a technology and business strategist there. He designed and tested network security tools, worked on security policy and standards, and headed company-wide security initiatives.

But entrepreneurship beckoned again, and in 2003 he became chief scientist at the start-up CounterStorm, which focuses on network-based detection of cyberthreats and malware. "Building enterprises from scratch has always been a big part of my career," he says.

When CERT approached him in 2010, he knew it was the perfect opportunity to not only apply his varied experience but also have a big impact on cybersecurity. He spends half his time at CERT in Pittsburgh and a quarter of it in Washington, D.C., in meetings with government agencies including the National Science Foundation, the Defense Advanced Research Projects Agency, and the Department of Homeland Security. The rest of the time he's on the road, traveling to conferences and government labs. "A big part of what I do is travel," he says. "My workdays are often unpredictable." ◆

Part-time Passions

Dan Olsen

Addressing the Disc

IEEE SENIOR MEMBER Dan Olsen remembers the first time he played disc golf, a competitive sport akin to traditional golf but one that uses Frisbee-like discs instead of clubs and balls. It was 1980, and he was a freshman at Oklahoma State University, in Stillwater, when friends took him to a course near Boomer Lake, two miles north of the school.

"I was hooked," says Olsen, now a power systems engineer with Shermco Industries, an electrical distribution and renewable energy services company, in Tulsa, Okla.

Each player traverses a 9- or 18-"hole" course, throwing a disc toward a hole and then picking it up from where it lands and throwing it farther. The goal is to get the disc into an elevated metal basket at each hole in the fewest throws possible. As with regular golf, the ultimate achievement is an ace, or hole-in-one.

Discs come in multiple styles—the edges are shaped differently to tailor the performance—and weights, mimicking golf's long-range drivers, midrange clubs, and short-range putters.

Olsen picked up the sport quickly and soon started playing in tournaments. Compared with traditional golf, he says, disc golf is more fun and intuitive. "And with disc golf," he adds, "the improvement of one's skills is exponential."

Elements of physics are involved, he points out. You have to factor in the weight of the disc, the rating factor—which is a measure of the speed, glide, and turn of the disc—and the wind. If you get the wind behind the disc, it tends to dip and head for the ground. But if it heads into the wind, it will lift, he explains, adding, "You don't want it to lift up too fast or it will end up in a tree."

In 1996, Olsen joined the Professional Disc Golf Association. He has gone from PDGA novice to Advanced Master, a category for players older than 40. He is now 54 and plays in the Amateur Division. In the three decades since he began, disc golf's popularity has boomed, especially in Oklahoma and Texas, he says. The PDGA has gone from more than 10,000 members at the time he joined to 60,000-plus.

Olsen plays disc golf with his friends after work for about four hours a week. He plays with his two grown sons when they visit. And he looks for a course wherever he travels for business. "I play whenever I can," he says. "If I'm not walking the dog, I'm walking the course. That's my exercise and one of my main stress relievers."

He competes in six to eight local and national tournaments per year. It costs about US $50 to enter, he says, and winners get cash or merchandise vouchers. A top tournament prize averages $18,000.

His best win was in the Texas State Doubles tournament in 1998, he says. More recently, he finished second in the Seminole Nation Days tournament in September in Wewoka, Okla.

Olsen figures that between gear, participation fees, and travel, he spends a few hundred dollars per year on the sport. "It's much less expensive than traditional golf," he says, "even though you end up losing some discs in the ponds and bushes."

—Prachi Patel

TY SAUNDERS

IEEE Senior Member Dan Olsen plays disc golf, a game in which players throw a Frisbee-like disk into an elevated metal basket in the fewest possible tries. As with regular golf, the goal is to get an ace, or hole-in-one.

John Moore

Retro Radios

WHEN IEEE MEMBER John Moore was 16, he used *The Radio Amateur's Handbook* to make a converter for his aunt's television that tuned it to channels outside its normal range. His love for such projects stayed with him. Now 71 and semiretired, he is a dedicated member of the Duxford Radio Society—a volunteer association of communications specialists who restore and repair donated radio equipment from both world wars for Duxford's Imperial War Museum, near Cambridge, England.

Moore, a history buff and born tinkerer, discovered vintage equipment later in life. He was captivated when he visited the museum in 2010 for the first time: "I trotted in one Sunday and said, 'What can I do to help?' Someone on staff told me the society just got a radio receiver and asked if I could get it going. I took it away and got it to work."

He currently is helping to fix an original H2S radar system. Invented by the British during World War II, it was the first airborne ground-scanning radar. He plans to interface it with a computer so that it can be driven by a simulator.

Moore goes to the museum once or twice a month, and he spends about four hours a week in his home workshop fixing receivers and transmitters. "It's quite a thrill to take home nearly irreplaceable equipment and get it to operate again," he says. "Finding what's wrong is like detective work." Sometimes he rebuilds the donated equipment from scratch. He hunts down obsolete

components—like diodes, inductors, capacitors, and tubes—from vintage radio stores, websites, and other radio societies. For repair instructions, he pores through old wartime publications. *Wireless for the Warrior*, a set of technical reference books for old British Army radio equipment, is his mainstay. He is thinking of replicating hard-to-find items like multipin connectors with a 3-D printer.

Moore considers himself fortunate, he says, that his engineering career links with his passion. He has designed and built computer monitors for International Computers Ltd., a large, now-defunct British manufacturer, as well as TV monitors for Prowest Electronics. In 1987, he helped found a start-up, Manitron Displays, which made the first compact radar screens. He left Manitron to start a consultancy in 1989 for flight simulators and 3-D displays.

In 1992, at the age of 48, he earned a Ph.D. in electrical engineering from the University of Cambridge, and he has since worked part time at its Centre for Advanced Photonics and Electronics while continuing his consulting work. The wealth of knowledge shared by the members of the Duxford Radio Society is exhilarating, he says. "You're forever learning new things," he adds. But the most rewarding part is demonstrating the radios to visitors. He recalls showing children how to use the radios in a mock-up of a British Lancaster bomber of World War II fame. "You can set the scene for them," he says. "How cramped it was; how, if you forgot to take your oxygen supply to the plane's bathroom, you could pass out. It really gives them a big charge." —*P.P.*

JOHN MOORE

The vintage radio gear that IEEE Member John Moore tinkers with at the Duxford Imperial War Museum, outside Cambridge, England, dates back to World War I.

OF NOTE

2015 Election Countdown

A look at open positions and deadlines

ON 1 MAY, the IEEE Board of Directors is scheduled to announce the candidates to be placed on this year's ballot for the annual election of officers, which will begin on 17 August. Those elected will take office next year. The ballot includes candidates for IEEE president-elect, who are nominated by the board, as well as nominees for delegate-elect/director-elect openings submitted by their respective division and region nominating committees.

The ballot also includes nominees for president-elect of the IEEE Standards Association and the members-at-large of its board of governors; vice president–elect, IEEE Technical Activities; and president-elect and member-at-large, IEEE-USA.

IEEE members who want to run for an office but have not been nominated need to submit a petition to the IEEE Board of Directors. The petition must include the necessary number of valid voting members' signatures, and the petitioner must meet other requirements as well. Petitions should be sent to the IEEE Operations Center, in Piscataway, N.J. The IEEE Board of Directors is also responsible for placing any proposed constitutional amendments on the ballot.

For more information about the process for getting on the ballot, visit the IEEE annual election Web page (http://www.ieee.org/election) or write to elections@ieee.org.

UP FOR ELECTION IN 2015

Chosen by all voting members
- IEEE president-elect

Chosen by members of all technical societies
- IEEE Technical Activities vice president–elect

Chosen by members of the respective technical divisions
- IEEE Division II delegate-elect/director-elect
- IEEE Division IV delegate-elect/director-elect
- IEEE Division VI delegate-elect/director-elect
- IEEE Division VIII delegate-elect/director-elect
- IEEE Division X delegate-elect/director-elect

Chosen by members of the respective regions
- IEEE Region 1 delegate-elect/director-elect
- IEEE Region 3 delegate-elect/director-elect
- IEEE Region 5 delegate-elect/director-elect
- IEEE Region 7 delegate-elect/director-elect
- IEEE Region 9 delegate-elect/director-elect

Chosen by members in Regions 1–6
- IEEE-USA president-elect
- IEEE-USA member-at-large

Chosen by members of the IEEE Standards Association
- Standards Association president-elect
- Standards Association board of governors members-at-large

DEADLINES AT A GLANCE

15 March Deadline for organizational units to submit slates of candidates to the IEEE Board of Directors for inclusion on the annual election ballot.

15 April Deadline for submitting an intention to file a petition to run for an office on the annual election ballot.

1 May IEEE Board of Directors submits to the voting membership a list of nominees for IEEE president-elect, delegate-elect/director-elect, as applicable, and other positions to be elected by voting members for the term to come. The board also announces whether it intends to put forward any constitutional amendments.

8 May Signed petitions nominating an individual for placement on the annual election ballot must be received by noon EDT USA/16:00 UTC.

17 August Annual election ballots are sent to all voting members on record as of 30 June. Voters may also begin accessing their ballots electronically.

1 October Marked ballots must be received by 1 p.m. EDT USA/17:00 UTC.

The 2014 Election Results

Here is the Tellers Committee's tally of votes counted in the 2014 annual election and approved in November by the IEEE Board of Directors.

IEEE President-Elect, 2015

Barry L. Shoop	15,972
Tariq S. Durrani	14,831
Frederick C. Mintzer	14,056

IEEE Division Delegate-Elect/Director-Elect, 2015

Division I	
Maciej J. Ogorzalek	1,358
Rakesh Kumar	1,154
Renuka P. Jindal	947
Division III	
Celia L. Desmond	3,651
Vijay K. Bhargava	3,635
Division V	
Harold Javid	3,011
Paolo A. Montuschi	2,952
Division VII	
Alan C. Rotz	2,498
John J. Paserba	1,907
Division IX	
K.J. Ray Liu	2,527
René M. Garello	2,236

IEEE Region Delegate-Elect/Director-Elect, 2015–2016

Region 2	
Katherine J. Duncan	2,010
Carole C. Carey	1,251
Region 4	
Bernard T. Sander	1,599
Hamid Vakilzadian	721
Region 6	
Kathleen A. Kramer	4,244
Sundaram K. "S.K." Ramesh	1,100
Region 8	
Margaretha A.K. Eriksson	5,027
Magdalena Salazar-Palma	5,013
Region 10	
Kukjin Chun	4,540
Stefan G. Mozar	3,248
Chun Che "Lance" Fung	3,093

IEEE Standards Association Board of Governors Member-at-Large, 2015–2016

Mark Epstein	523
Philip C. Wennblom	452
Dennis B. Brophy	336

IEEE Standards Association Board of Governors Member-at-Large, 2015–2016

Glenn W. Parsons	611
Alexander D. Gelman	365
Oleg Logvinov	334

IEEE Technical Activities Vice President–Elect, 2015

José M.F. Moura	14,083
Douglas N. Zuckerman	13,991

IEEE-USA President-Elect, 2015

Peter Alan Eckstein	11,680
Keith D. Grzelak	8,624

IEEE-USA Member-At-Large, 2015–2016

Scott M. Tamashiro	12,506
Gim Soon Wan	7,790

ISTOCKPHOTO

Introducing the 2015 Class of Fellows

The Institute congratulates these 300 IEEE senior members named IEEE Fellows for 2015. They join an elite group of people who have contributed to the advancement or application of engineering, science, and technology.

David Kazuo Abe
Vivek Agarwal
Héctor Jorge Altuve-Ferrer
Daniel Matthew Andrews
David Angeli
Jean Armstrong
David I. August
Christopher P. Auth
Randy Keith Avent
Anastasios G. Bakirtzis
Gerhard A. Bauch
Jason R. Baumgartner
Randal W. Beard
Wiren Dale Becker
Kristine L. Bell
Ewert Bengtsson
Charanjit Singh Bhatia
Ricardo Bianchini
Marcela Milena Marie Bilek
Kenneth Paul Birman
Daniel Wesley Bliss
Aaron Fred Bobick
Nuno Borges Carvalho
Alberto Borghetti
Olga Boric-Lubecke
Azzedine Boukerche
Victor M. Bright
Martin George Buehler
Wolfram Burgard
Rajkumar Buyya
Christian Cachin
Ning Cai
Natalino Camilleri
Jiannong Cao
Paolo Carbone
Joseph R. Cavallaro
Chandan Chakraborty
Elizabeth Jiang Chang
Biao Chen
Chi-Chih Chen
Xiaodong Chen
Ming Cheng
Xiuzhen Cheng
Howie M. Choset
Jyh-Horng Chou
Henrik I. Christensen
Chen-Nee Chuah
Mooi Choo Chuah
Israel Cohen
Iain Bruce Collings
John F. Conley
Javier Contreras
Jordi Cortadella
Tie Jun Cui
John Michael Dallesasse
Sajal K. Das
Dipankar Dasgupta
Purnendu Kumar Dasgupta
Michael Evan Davies
Mérouane Debbah
Joe Charles Decuir
Lieven De Lathauwer
Francisco de León
Michael Demetriou
Laurent Pierre Desclos
Murthy Devarakonda
Peter August Dinda
Edward John Dobrowolski
Rolf Drechsler
Josef Cenek Drobnik
Jeffrey L. Duerk
Alistair Paul Duffy
Frank Joseph Effenberger
Carl August Ekdahl Jr.
Randy E. Ellis
Dara Entekhabi
Babak Fahimi
Pingzhi Fan
Weileun Fang
Lorenzo Faraone
Ernest Joseph Feleppa
Alan Simon Finkel
William R. Finley
Michael Paul Fitz
Michael Patrick Flynn
Kenneth G. Foote
Stephanie Forrest
Dieter Fox
Gordon John Frazer
Henry Fuchs
Pascale Fung
Xiqi Gao
Reza Ghodssi
Amitava Ghosh
Monisha Ghosh
Patrick Girard
Nachappa Gopalsami
Manimaran Govindarasu
Robert Ian Gresham
Min Gu
Josep M. Guerrero
Guna Seetharaman Gunasekaran
Deepnarayan Gupta
Dan M. Gusfield
John Bruce Hacker
Paul David Hale
Dan Halperin
K.V.S. Hari
Zhihai He
Constance Louise Heitmeyer
Abdelsalam Ali Helal
Jöerg Henkel
Gary Robert Hoffman
Toshikazu Hori
Ray-Hua Horng
John Alexander Hossack
Ekram Hossain
Jianying Hu
Yi Hu
Howard Cheng Huang
Giuseppe Iannaccone
Meikei Ieong
Makoto Iwasaki
Ravishankar R. Iyer
Qiang Ji
Hong Jiang
Hong Jiang
Nihar Jindal
James Arthur Jodice
Richard Darryl Jones
Anupam Joshi
Tzyy-Ping Jung
Mohan V. Kalkunte
Safa Kasap
Young-Han Kim
Youngky Kim
Tsunenobu Kimoto
Simon Alistair King
Stefanos D. Kollias
Hiroshi Kondoh
Christoforos Kozyrakis
David J. Kriegman
Deepa Kundur
Hao-chung Kuo
Gérard Lachapelle
Sanjay Gouri Lall
Edmund Y. Lam
Christian Laurent
Paul Ren Lecoq
Paul P. Lee
Thomas H. Lee
Henry K. Leung
Steven Peter Levitan
Baochun Li
Keqin Li
Ming-Jun Li
Xiang-Yang Li
Daniel Lidar
Cheng-Lin Liu
Ling Liu
Yong Liu
Yunhao Liu
Zicheng Liu
John Robert Long
Susan M. Lord
Wenjing Lou
David James Love
Jianhua Lu
David L. Lubkeman
Giuseppe Macchiarella
Abhijit Mahalanobis
Scott A. Mahlke
Dragan Maksimovic
Roger John Malik
Debendra Mallik
Diana Marculescu
Detlev Marpe
Sylvain M. Martel
Luis Marti
Yehia Massoud
Witold Piotr Maszara
Paolo Mattavelli
Gianluca Mazzini
Stephen J. McArthur
Timothy John McCoy
Patrick D. McDaniel
Hong Mei
Shengwei Mei
Jean-Pierre Merlet
Mehran Mesbahi
Ethan L. Miller
Stefan Gerhard Mozar
Boris Murmann
Tadao Nagatsuma
Krishna Rama Narayanan
Paul Michael Newman
Khai Doan The Ngo
Alexandru Nicolau
Tetsuji Oda
Kiyoshi Ohishi
Michael E. Orshansky
Marek A. Osinski
Philip Norman Overholt
Teresa Pace
Sokrates Theodore Pantelides
Unnikrishna Pillai
Antonio J. Plaza
Mark D. Plumbley
David J. Pommerenke
Radha Poovendran
Mircea Popescu
Robert Caiming Qiu
Bhaskar Ramamurthi
Sundaram K. Ramesh
John Neal Randall
Spiridon A. Reveliotis
David John Richardson
Rasheek M. Rifaat
Eric Rotenberg
Ahmed A. Rubaai
Markus Rupp
Ponnuswamy Sadayappan
Safieddin Safavi-Naeini
Robert James Safranek
Surya Santoso
Richard Schreier
Luca Selmi
Michael C. Shebanow
Peng Shi
James D. Shields
Yoshihiro Shiroishi
Moshe Shoham
Mario G. Silveirinha
Gail Skofronick-Jackson
Paris Smaragdis
Peter Jeffrey Smith
Hing Cheung So
Haruhisa Soda
William S. Song
Charles W. Stearns
Eckehard Goetz Steinbach
Gregory Edward Stewart
Stefano Stramigioli
Suresh Subramaniam
Ponnuthurai Nagaratnam Suganthan
Dong Sun
Jian Sun
Yu Sun
Dan Keun Sung
Wonyong Sung
Johan A. K. Suykens
Dacheng Tao
Paul J. Tasker
David Taubman
Fernando Lisboa Teixeira
Rajeev Thottappillil
Yuichi Tohmori
Ridha Touzi
Harry L. Trentelman
James Joseph Truchard
Masashi Usami
Vesa Valimaki
Son Van Nghiem
John Thomas Vaughan
Vaithianathan Venkatasubramanian
Michel Verleysen
Mahesh Viswanathan
Yurii A. Vlasov
Alexander Waibel
Jian-Ping Wang
Geoffrey Ian Webb
Mark H. Weichold
David Mandel Weiss
Dieter J. Weller
Blake Shaw Wilson
An-Yeu Wu
Hsiao-Chun Wu
Ji Wu
Gaozhi George Xiao
Xiaolan Xie
Yuan Xie
Isao Yamada
Liuqing Yang
Olexander Georgiyovych Yarovyi
Aylin Yener
Bulent Yener
Wang Yi
Chik Patrick Yue
Moti Yung
Navid Reza Zargari
Huaguang Zhang
Wei Zhang
Wei-Bin Zhang
Yin Zhang
Yong-Hang Zhang
Zhijun Zhang
Haitao Zheng
Yahong Rosa Zheng
Kun Zhou
Yuanyuan Zhou

RANDI KLETT

Nominations Sought for Leaders in 2016 and 2017

Volunteers are needed to serve as corporate officers, committee chairs, and more

IEEE IS GOVERNED by volunteer members and depends on them for many things. For example, they edit IEEE publications, organize conferences, coordinate regional and local activities, write standards, lead educational activities, and identify individuals for IEEE recognitions and awards.

The Nominations and Appointments (N&A) Committee is responsible for developing recommendations for staffing many volunteer positions, including candidates for president-elect and corporate officers. Its recommendations are sent to the IEEE Board of Directors and the IEEE Assembly. Accordingly, the N&A Committee is seeking nominees for the following positions:

2017 IEEE President-Elect (who will serve as president in 2018)

2016 IEEE Corporate Officers

- Vice president, Educational Activities
- Vice president, Publication Services and Products
- Secretary
- Treasurer

2016 IEEE Committees (chairs and members)

- Awards Board
- Employee Benefits and Compensation
- Ethics and Member Conduct
- Fellow
- Governance
- History
- Nominations and Appointments
- Public Visibility
- Tellers

DEADLINE FOR NOMINATIONS

15 March 2015

WHO CAN NOMINATE?

Anyone may submit a nomination; nominators do not need to be IEEE members, but nominees must meet certain qualifications. Self-nominations are encouraged. An IEEE organizational unit may submit recommendations endorsed by its governing body or the body's designee.

A person may be nominated for more than one position. Nominators need not contact their nominees before submitting the form. The N&A Committee will contact them to determine their eligibility and willingness to serve.

HOW TO NOMINATE

For information about the positions, including qualifications and estimates of the amount of time required during the term of office, check the Guidelines for Nominating Candidates at http://www.ieee.org/about/corporate/nominations/nominations_guidelines.html. To nominate a person for a position, complete the online form.

NOMINATING TIPS

Positions for which the N&A Committee makes recommendations represent the uppermost governance levels in IEEE. Volunteers with relevant prior experience in lower-level IEEE committees and units are recommended by the committee more often than volunteers without such experience. For example, candidates for the IEEE Awards Board have a greater likelihood of being recommended if they have already served on an awards committee of a society, section, or region or on another IEEE board.

It is also helpful to check eligibility requirements at the N&A Committee website at http://www.ieee.org/nominations before submitting a nomination to avoid submitting an ineligible candidate.

Individuals recommended for president-elect and corporate officer positions are more likely to be recommended if they have a strong record of leadership and accomplishment within and outside IEEE. Recommended candidates often have significant prior experience on IEEE boards and committees.

More information about the duties of the different positions, qualifications, and eligibility requirements (such as prior service in certain positions or IEEE grades) can be found in the Guidelines for Nominating Candidates.

—Peter W. Staecker, Chair
2015 IEEE Nominations and Appointments Committee